



## A Survey on Credit Card Fraud Detection using Deep Learning Model

Mrs. R. Jayalakshmi<sup>1</sup>, Dr. R.G. Suresh Kumar<sup>2</sup>, Thanushree T<sup>3</sup>

<sup>1</sup>Assistant professor, Department of CSE, Rajiv Gandhi College of Engineering and Technology, Puducherry, India.

<sup>2</sup>Head of the Department, Department of CSE, Rajiv Gandhi College of Engineering and Technology, Puducherry, India.

<sup>3</sup>UG Scholar, Department of CSE, Rajiv Gandhi College of Engineering and Technology, Puducherry, India.

**Emails:** jayalakshmi\_r@rgcet.edu.in<sup>1</sup>, sureshkumar\_rg@rgcet.edu.in<sup>2</sup>, thanushree1701@gmail.com<sup>3</sup>

### Abstract

The research evaluates all recent applications of machine learning (ML) and deep learning (DL) for detecting credit card fraud. The study details multiple approaches to develop fraud detection systems by exploring both data quality enhancement methods along with feature selection approaches and modeling strategies. The implementation of advanced deep learning approaches LSTM together with CNNs leads to high real-time detection of fraud because they excel at detecting sophisticated temporal sequences. XGBoost ensemble methods used with AdaBoost and SMOTE methods make great strides in improving fraud dataset handling of class imbalance issues. The method which is known as federated learning currently attracts attention because it helps institutions to collaborate on separate model training without exposing their actual data. Problems persist with the current development of fraud detection models since they need adaptable models for various datasets while also requiring interpretation capabilities and functionality that adapts to changing deceit patterns. The development of privacy-preserving methods for fraud detection must continue because they need to achieve sufficient efficiency and security standards for real-time applications. Problems with scalability in addition to unclear detection methods and adaptability require new research directions that fill existing knowledge gaps.

**Keywords:** Credit Card Fraud Detection; Deep Learning; Ensemble Learning; Machine Learning.

## 1. Introduction

### 1.1 Background

The digital era considers credit card fraud to be an established financial crime that causes substantial economic damage worldwide. E-commerce and mobile payment expansion requires more frequent credit card utilization which creates new possibilities for counterfeiters to take advantage of payment systems flaws. According to the Nilson Report, credit card fraud losses on a global scale reached the mark of USD 31 billion in 2020 and are likely to surge owing to the rising intricacy of such types of frauds (Sulaiman, R.B et al., 2022). Fraudsters always found ways to bypass traditional security measures so it is more important now to have advanced detection techniques (Mienye, I.D et al., 2024). Credit card fraud detection focuses on identifying anomalies beyond typical user behavior. Due to high transaction volumes, machine learning and deep learning methods surpass rule-based systems by efficiently processing large datasets in real time (Alarfaj, F.K et

al., 2022; Khalid, A.R et al., 2024). CNNs and LSTMs effectively analyze transaction sequences, identifying hidden fraud patterns in complex data streams (Alfaiz, N.S et al., 2022; Esenogho, E et al., 2022).

### 1.2 Challenges in Fraud Detection

Despite the advancements in fraud detection, several challenges remain:

- **Class Imbalance:** Fraudulent transactions are rare, causing models to favor non-fraudulent cases, leading to false negatives.
- **Data Privacy:** Regulations like GDPR and HIPAA complicate data sharing, with federated learning offering a privacy-preserving solution.
- **Evolving Fraud Techniques:** Fraudsters continually adapt, requiring advanced methods like unsupervised learning and ensemble models to detect new fraud patterns.

### 1.3 Research Questions

This paper explores key research questions:

- How can hybrid modeling and ensemble methods address class imbalance in fraud detection?
- How do base model combinations like XGBoost and LightGBM enhance detection accuracy?
- How do preprocessing techniques, including feature extraction and resampling with SMOTE and autoencoders, improve model performance?
- How can federated learning ensure data privacy while maintaining effectiveness in multi-institution fraud detection?

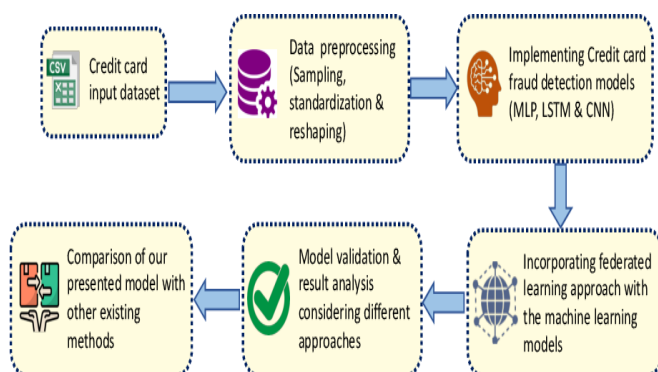
### 1.4 Importance of Advanced Techniques

Advanced techniques like CNNs, LSTMs, and autoencoders enhance fraud detection by recognizing intricate patterns in high-dimensional data. Stacking ensemble models outperform individual classifiers (Jovanovic, D et al., 2022; Xiang, S et al., 2023). Unsupervised methods, including anomaly detection and GANs, help identify fraud without relying on extensive labeled data (Mniai, A et al., 2023; Salam, M.A et al., 2024).

## 2. Literature Overview

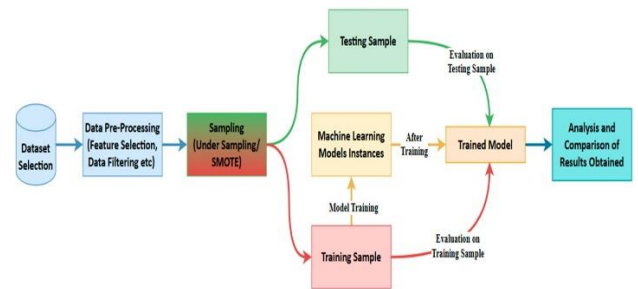
### 2.1 Machine Learning Approaches in Credit Card Fraud Detection

Research on credit card fraud detection shows that ensemble methods like AdaBoost and XGBoost enhance performance on imbalanced datasets (Sulaiman, R.B et al., 2022). Federated learning further improves detection by enabling secure, collaborative model training, Figure 1.



**Figure 1 Federated Learning Process for Credit Card Fraud Detection Across Banks [1]**

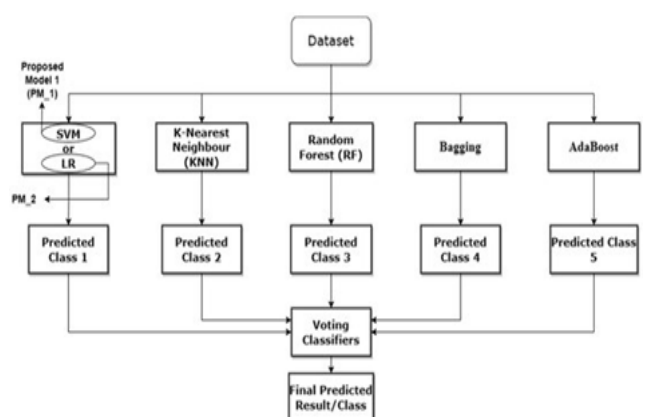
Mimanye and Jere (2024) two other models reviewed several ML algorithms, whose major shortcoming is their performance on structured data, whereby their accuracy lags in detecting new fraud patterns requiring further well-trained sophisticated techniques (Mienye, I.D et al., 2024), as shown in Figure 2.



**Figure 2 Flow Diagram of Credit Card Fraud Detection Using Machine Learning [2]**

### 2.2 Deep Learning Techniques in Fraud Detection

Fraud detection has gained popularity due to its ability to automate feature extraction. Deep Neural Networks (DNNs) utilize Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) for sequence modeling. Khalid et al. (2024) demonstrated that LSTMs effectively track fraud patterns, outperforming traditional ML models (Alarfaj, F.K et al., 2022), Figure 3.



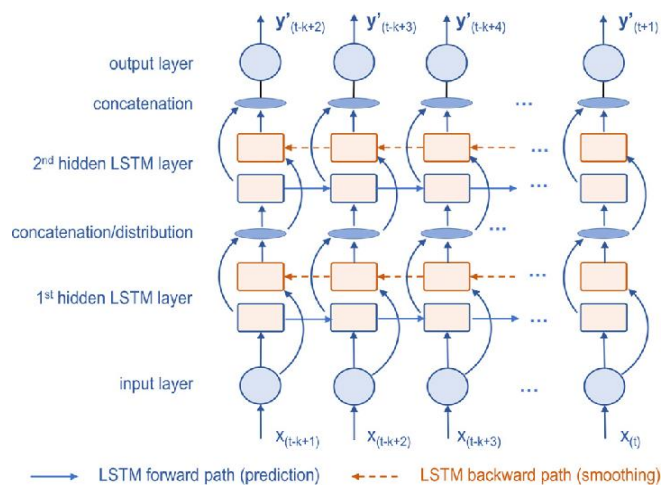
**Figure 3 An Ensemble Model Using Multiple Classifiers for Fraud Detection, with a Final Predicted Result Based on Voting [3]**

Ensemble methods improve accuracy by combining multiple classifiers. Neural network ensembles

enhance detection in complex datasets (Khalid, A.R et al., 2024), while deep CNNs effectively identify hidden fraud patterns (Alfaiz, N.S et al., 2022).

### 2.3 Hybrid Models and Ensemble Learning

Ensemble learning and hybrid models enhance fraud detection by combining multiple algorithms for superior predictive accuracy. Research shows that stacking and boosting techniques integrate different models into advanced solutions. Mienye and Sun (2023) achieved improved fraud detection using a deep learning ensemble with data resampling, outperforming single models (Esenogho, E et al., 2022). Figure 4 illustrates a hybrid ensemble incorporating LSTM and GRU, with an MLP meta-classifier for final fraud prediction, enabling better pattern recognition [4-5].



**Figure 4 A Stacked Ensemble Model Combining LSTM And GRU Base Models with an MLP Meta-Classifier for Fraud Detection [6]**

Tiwari et al. (2021) demonstrated that combining AdaBoost with SVM significantly improves classification accuracy, particularly in imbalanced datasets, addressing a common challenge in fraud detection (Ileberi, E et al., 2022), Figure 4.

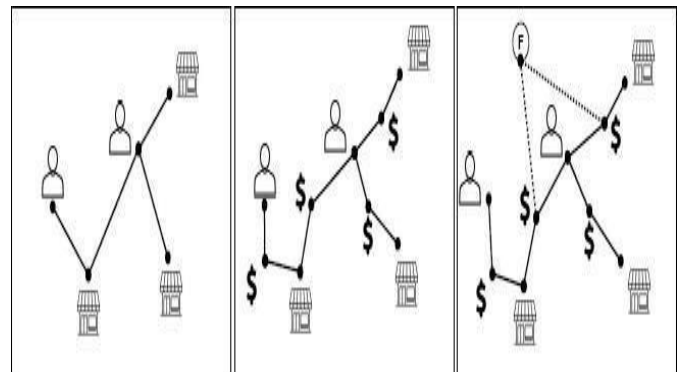
### 2.4 Addressing Class Imbalance and Data Privacy

Fraud detection datasets often face class imbalance due to the rarity of fraudulent transactions, which techniques like SMOTE and undersampling help address. Salekshahrezaee et al. (2023) found that combining Convolutional Autoencoders (CAEs) with SMOTE yielded the best F1-score and AUC for fraud

detection (Asha, R. B et al., 2021). Additionally, federated learning enables secure collaboration between institutions without sharing raw data. Abdul Salam et al. (2024) demonstrated how this approach enhances fraud detection while maintaining data privacy across multiple organizations (Cherif, A et al., 2023).

### 2.5 Advanced Techniques: Unsupervised Learning and Anomaly Detection

Unsupervised learning is increasingly used in fraud detection to identify new patterns without labeled data. Techniques like GANs and autoencoders aid in anomaly detection. Van Belle et al. (2023) proposed a node representation learning method for analyzing transaction relationships without supervision (Ileberi, E et al., 2021). Likewise, Jiang et al. (2023) developed an Unsupervised Attentional Anomaly Detection Network using autoencoders and GANs for improved fraud detection accuracy (Tiwari, P et al., 2021), Figure 5 [7-9].



**Figure 5 Left: Bipartite Graph with Cardholders and Merchants. Middle: Tripartite Graph with Transactions as Nodes. Right: A 'Fraud' Node is Added to Connect Fraudulent Transactions [10]**

### 2.6 Hybrid Models and Ensemble Methods for Improved Accuracy

Ensemble and hybrid models improve fraud detection by addressing class imbalance and complex patterns. Mienye and Sun (2023) enhanced accuracy using LSTMs with SMOTE (Chen, J.I.Z et al., 2021). Tiwari et al. (2021) combined SVM and XGBoost to reduce bias in high-dimensional data (Gupta, P et al., 2023). Esenogho et al. (2022) showed that neural network ensembles with feature engineering further boosted accuracy (Khalid, A.R et al., 2024).



## 2.7 Advanced Deep Learning Models for Sequential Fraud Detection

Deep learning models like LSTMs and RNNs excel in detecting fraud in sequential financial data. Banchaji et al. (2021) developed an LSTM with an attention mechanism to highlight key transaction features, enhancing fraud detection through feature selection and dimension reduction (Mienye, I.D et al., 2023) [11-13].



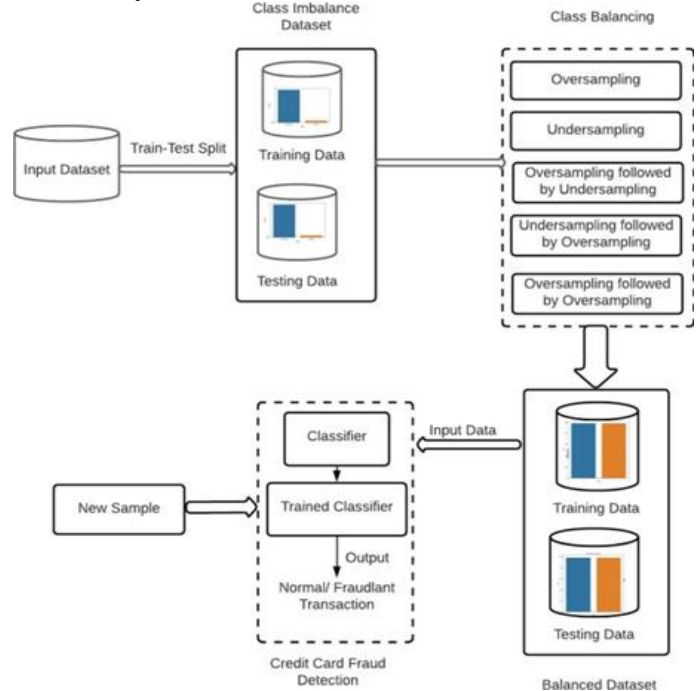
**Figure 6** Architecture of The Proposed Credit Card Fraud Detection Model with LSTM and Attention Mechanism [14]

Yu et al. (2024) showed that transformers outperform RNNs and LSTMs in detecting fraud by capturing long-range dependencies (Belle, R.V et al., 2023). Mniai (2023) combined CNNs and LSTMs to develop a scalable hybrid model for enhanced fraud detection (Benchaji, I et al., 2021), Figure 6.

## 2.8 Federated Learning for Privacy-Preserving Fraud Detection

Federated learning enables secure, collaborative fraud detection by training models on decentralized data without sharing raw information. Abdul Salam et al. (2024) found this approach enhances model accuracy while ensuring compliance with privacy regulations like GDPR and HIPAA (Yu, C et al., 2024). Figure 7 illustrates federated learning in fraud detection, where institutions collaborate without sharing sensitive data. Abdul Salam et al. (2024) found that this approach enhances model performance while ensuring GDPR and HIPAA compliance. Integrating differential privacy techniques further secures individual data, making federated learning a key solution for fraud detection

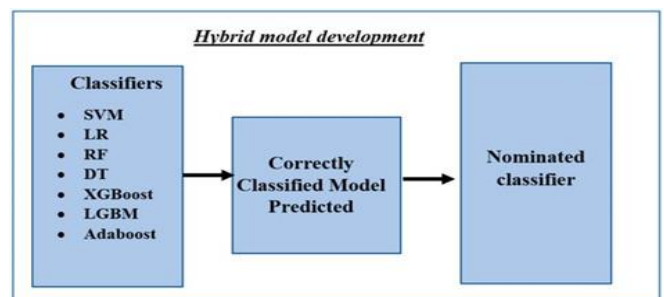
in regulated sectors like banking and healthcare (Noviandy, T.R et al., 2023) [15-16].



**Figure 7** Federated Learning Process for Credit Card Fraud Detection [17]

## 2.9 Real-Time Detection and Scalability Challenges

With the rise in credit card transactions, quick fraud detection is crucial to prevent financial losses. Researchers focus on developing scalable models while ensuring system efficiency. Deep learning models like CNNs and LSTMs excel in real-time fraud detection by identifying complex patterns in sequential transaction data [18].



**Figure 8** Hybrid Model for Real-Time Fraud Detection Using Multiple Classifiers [19]

Malik et al. (2022) developed a hybrid fraud detection model combining SVM, XGBoost, and

real-time processing, ensuring scalability with minimal inaccuracies (Jovanovic, D et al., 2022). Figure 8 illustrates this model, which adapts to evolving transactions using streaming data and online learning. Similarly, Lin and Jiang (2021) applied autoencoders and probabilistic random forests to detect emerging fraud patterns in dynamic transaction environments (Xiang, S et al., 2023).

## 2.10 Addressing Class Imbalance in Fraud Detection

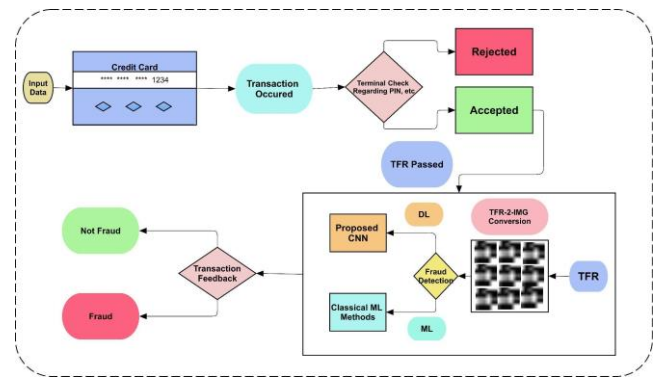
Fraud detection faces challenges due to class imbalance. Salekshahrezaee et al. (2023) showed that SMOTE and undersampling improve model performance by reducing bias toward the majority class (Mniai, A et al., 2023). Jovanovic et al. (2022) enhanced fraud detection accuracy by applying a group search firefly algorithm to XGBoost, particularly when combined with SMOTE (Salam, M.A et al., 2024). These techniques are crucial for building unbiased fraud detection systems.

## 2.11 Advanced Approaches for Handling Class Imbalance

Class imbalance in fraud detection remains a challenge due to the rarity of fraudulent transactions. Singh et al. (2022) found that combining SMOTE with AdaBoost improved accuracy and recall while reducing bias toward the majority class (Salam, M.A et al., 2024; Salekshahrezaee, Z et al., 2023). Addressing this imbalance is essential for building an effective fraud detection system.

## 2.12 Federated Learning and Privacy-Preserving Fraud Detection

Federated learning enables institutions to collaborate on building fraud detection models without sharing raw data, ensuring privacy compliance with regulations like GDPR. Abdul Salam et al. (2024) demonstrated that federated learning enhances fraud detection while maintaining data privacy, making it a viable approach for financial applications (Zhu, M et al., 2024). Similarly, Alharbi et al. (2022) used deep learning with federated learning, allowing models to learn from distributed datasets without exposing sensitive customer data, further ensuring privacy preservation (Jiang, S et al., 2023). As shown in Figure 9, transaction data is transformed into an image-like format, enabling privacy-preserving learning across distributed datasets [20-24].



**Figure 9 Text2IMG Mechanism for Transforming Transaction Data into Images for Fraud Detection [25]**

## 2.13 Real-Time Fraud Detection and Scalability

Scalable models capable of processing large volumes of transaction data efficiently are essential for real-time fraud detection. Yu et al. (2024) introduced an enhanced transformer model that outperforms traditional LSTM and CNN models in handling large datasets and identifying long-range dependencies in transaction data, making it ideal for real-time fraud detection (Malik, E. F et al., 2022). Novianidy et al. (2023) demonstrated that XGBoost, combined with data augmentation, can effectively detect fraudulent transactions in time-series data, providing a scalable solution for financial institutions processing millions of transactions daily (Habibpour, M et al., 2023). These findings highlight the need for scalable, real-time models suitable for high-frequency transactions.

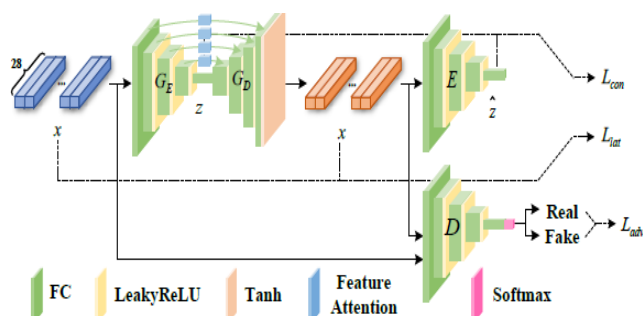
## 2.14 Uncertainty-Aware Models for Fraud Detection

Fraud detection is critical in this process as dynamic environments with evolving fraud patterns require good handling of uncertainty in predictions. Models with uncertainty awareness can produce confidence intervals for predictions which can help to reveal to what extent the model is reliable and diminish the risk of false positives. Monte Carlo dropout and ensemble techniques were used to estimate the uncertainty of the predictions of fraud, as proposed by Habibpour et al. (2023). Through this approach the model was able to detect potential fraudulent transactions based on low confidence score and the resulting help to better decision making and prevent the miss of fraudulent transactions (Alharbi, A et al., 2022). Furthermore, it was shown that fraud detection models can be made

more robust by the use of ensemble Monte Carlo dropout. The conclusion of the study stated that in high stakes domains like the one presented in the paper involving fraud detection, uncertainty quantification is necessary when decisions are made on low confidence predictions that could potentially lead to large financial losses. Fraud detection models can be made more reliable and trustworthy with uncertainty being integrated in the prediction process.

### 2.15 Hybrid Models for Real-Time Fraud Detection in Imbalanced Datasets

Combining traditional machine learning with deep learning enhances real-time fraud detection and addresses class imbalance. Malik et al. (2022) developed a hybrid model using SVM and XGBoost, improving accuracy by balancing fraud-related features in large-scale transaction data (Lin, T.H et al., 2021). Lin and Jiang (2021) integrated autoencoders with probabilistic random forests for real-time fraud detection, making their model effective for imbalanced datasets and dynamic financial environments. This approach improved detection speed, robustness, and energy efficiency (Singh, A et al., 2022). Figure 10 illustrates this framework, where autoencoders handle feature learning and random forests enhance decision-making [26-29].



**Figure 10 Framework for Fraud Detection Based on Unsupervised Attentional Anomaly Detection [30]**

## 3. Methodologies and Approaches

The different ways in which data was then collected, preprocessed and analyzed for methodologies approaches literature described in this section. These are methods that cover all the steps of data collection, data preprocessing, ML, and DL methods for detecting transactions that are fraudulent.

### 3.1 Data Collection Methods

Most of the studies in fraud detection use the transaction dataset from financial institutions or publicly available dataset i.e. Kaggle. The datasets typically contain key transaction merchant, location and the card holder information. There exist many studies that provide collaborative datasets collected from multiple institutions, e.g., (Yu, C et al., 2024). Federated learning provides the facility for decentralized data processing; that is, collaborative training of fraud detection models by several institutions without directly sharing sensitive data. There is no compromise on data privacy as this method respects privacy regulations such as GDPR and HIPAA, which is a critical aspect when working with financial datasets. The collaborative approach of ensuring that the data the fraud detection models are trained on consists of a variety of data improves the robustness and generalization ability.

### 3.2 Data Preprocessing Techniques

Fraud detection, however, relies on data preprocessing since without it, we don't have a suitable format of transaction data to feed into our machine learning models to make the predictions. The first step is data cleaning which consists of getting rid of irrelevant or missing data or if data has any inconsistencies, then handling them. Data imputation techniques which are used in several studies, such as (Esenogho, E et al., 2022), fill missing values so that the datasets can be processed by the models. Another crucial preprocessing step is feature engineering in which raw data is transformed to better features as that could increase the performance of the model. For example, (Alarfaj, F.K et al., 2022) applied the Principal Component Analysis (PCA) to decrease the dimensionality and to make the selection of features process more efficient, avoiding using unimportant features while training the model. This work can also provide normalization and standardization to features based on given ranges to some extent (if the features are not normalized and standardized, the study suggested that applying neural networks could be a problem in (Alarfaj, F.K et al., 2022)). These preprocessing techniques help us load the high and large dimensional datasets in such a way that models easily can process them. One crucial problem in fraud detection is the class



imbalance between the number of fraudulent transactions and the legitimate transactions. To attempt to keep the class balance, several studies such as (Yu, C et al., 2024) have used SMOTE (Synthetic Minority Over-sampling Technique) to create synthetic fraud cases. (Benchaji, I et al., 2021) and others have utilized undersampling methods to reduce the imbalance of the majority class (legitimate transactions) in an attempt to facilitate model learning of the fraudulent characteristics.

### **3.3 Data Analysis and Feature Selection**

Feature selection is very important in selecting the set of features that would be useful in enhancing model performance and avoiding overfitting. The studies employed in (Ileberi, E et al., 2022) used the genetic algorithms and (Khalid, A.R et al., 2024) they used the recursive feature elimination to discard features that are not relevant or redundant. These methods mitigate issues such that the features used are independent, not redundant, and are predictive of the model of fraud. Also, correlation analysis and mutual information techniques have been used in several studies to investigate the relation between different features to the target variable (fraud or not fraud). These techniques lead to reduction in dimensionality of the dataset and not including unnecessary (but irrelevant) features in the final model.

### **3.4 Machine Learning and Deep Learning Models**

As shown in (Sulaiman, R.B et al., 2022), these models are very good at learning the patterns from historical data regarding fraud. For instance, AdaBoost and XG boost are employed to increase the performance of these models in the way that these models make use of multiple classifiers in order to create so many types of ensemble that lead to increase in the accuracy and decrease in the over fitting. (Asha, R. B et al., 2021) and (Jovanovic, D et al., 2022) have studied that ensemble methods are very effective to deal with an imbalanced dataset where both predictions of fraudulent and non-fraudulent transactions can be done precisely. LSTMs are highly useful in catching the time dependency on transaction sequences and the ability to learn fraud patterns that change over time. (Mienye, I.D et al., 2024) and (Alarfaj, F.K et al., 2022) are two studies that utilize LSTM based models for fraud detection wherein it is

observed that these models are capable models in capturing long term dependencies in the transaction sequence and hence improve fraud detection accuracy. Moreover, some studies, e.g., (Alfaiz, N.S et al., 2022), have explored Convolutional Neural Networks (CNN) to learn relevant features automatically from raw transaction data directly without manually designing features as in the previous studies. Besides, hybrid models based on traditional ML algorithms as well as DL techniques have become popular. Based on the (Jovanovic, D et al., 2022), these models exploit the strengths of both approaches. For example, XGBoost combined with LSTM and SVM with CNN can provide an opportunity to boost the model performance by simultaneously making use of deep feature learning and ensemble boosting for increasing classification accuracy and building more resistant fraud detection systems.

### **3.5 Model Evaluation**

The literature uses different tests of performance fraud detection. It is common to report accuracy, but it is not a good measure of model performance, in particular, in imbalanced datasets. For fraud detection, therefore, it is very important that the predictions of frauds are accurate, and recall that the number of fraudulent transactions is maximised. It is often the case that the two metrics, them (Alarfaj, F.K et al., 2022; Khalid, A.R et al., 2024), when working with highly imbalanced data. Moreover, the AUC-ROC curve is applied for evaluating discrimination ability of the model identifying fraudulent and non-fraudulent transactions, and the closer AUC value to 1, the more successful the model is working. Another common way to ensure that model generalizes well and is robust is to use cross validation.

### **3.6 Real-Time Fraud Detection and Scalability**

A significant task in fraud detection is to guarantee that the system can process high frequency high volume transactions in real time. The studies tend to spend much effort on whether the models scale well in processing large datasets quickly while maintaining high accuracy. (Jovanovic, D et al., 2022) has shown that XGBoost and LightGBM have been used for real time fraud detection as these models can handle very large datasets and give accurate predictions in a short amount of time.

#### 4. Findings and Trends

These models can detect sequential and temporal dependencies present in sequences of transactions, which can help us detect a pattern of transactions that are likely to be a sign of evolving fraud activities at an early stage. According to (Mienye, I.D et al., 2024) and (Alfaiz, N.S et al., 2022), it is mentioned that these deep learning approaches perform very well for real time applications, for example towards fraud detection systems, especially when SMOTE or other class balancing approaches are included. Of second importance are ensemble learning methods where a group of smaller or simpler functions are combined. XGBoost and AdaBoost with such models as SVM or RF to combine has already shown some improvements of the fraud detection accuracy, but primarily works nicely with the imbalanced datasets. It is found that by mixing up the traditional machine learning technique and the deep learning, such hybrid models provide higher classification accuracy and improved robustness with respect to the traditional system because both have properties. Meanwhile the trend towards federated learning also has a momentum and this is so in the cases where the attention cannot be obscured from privacy concerns. Develop a model collaboratively among financial institutions, where none of these institutions are required to share their privacy risky transaction data, as demonstrated in (Yu, C et al., 2024).

#### 5. Challenges and Gaps

The fraud detection has been substantially improved; however, the existing studies also have some challenges and gaps. To be able to deal with cases like these, techniques such as SMOTE have been employed widely; however, the generated synthetic data might not represent the actual fraud patterns resulting in false positives or negatives. The second limitation in the literature is that the fraud detection models cannot be generalized. Many of the studies incur proprietary datasets or datasets that are not representative of the entire spectrum of fraud patterns. However, the scalability of the fraud detection models to detect real time fraud in large transaction volume without excessive trade-off to the accuracy when using the models are other problems. Hole in the literature also includes the model interpretability aspect. Shown to be superior in

performance, but they are sometimes black boxes because they are hard to intuitively understand how it reached back to a certain decision. The lack of transparency would be problematic in industries such as finance where stakeholders have reasons for regulation and operational. Secondly, privacy concerns are also an important issue. We have also investigated such other privacy preserving techniques as federated learning but no standardized security approaches for sharing models securely or anonymizing data without losing accuracy were introduced yet.

#### Conclusion

The survey demonstrates clear evidence that machine learning together with deep learning methods enhance credit card fraud detection but some remaining obstacles remain to be resolved. The detection process received upgrades through the incorporation of advanced models that use LSTM and CNN together with hybrid ensemble techniques to increase detection precision and manage class imbalance while maintaining real-time operation. The data privacy protection abilities of federated learning have been shown to operate effectively for building collaborative models. The current detection system continues to face two fundamental problems related to model interpretability as well as generalization capabilities across datasets alongside fraud pattern adaptation. Enhanced implementation of such areas along with improved privacy-protection methodologies should result in enhanced robustness as well as scalability and transparency for fraud detection systems.

#### References

- [1]. Bin Sulaiman, R., Schetinin, V., & Sant, P. (2022). Review of machine learning approach on credit card fraud detection. *Human-Centric Intelligent Systems*, 2(1), 55-68.
- [2]. Mienye, I. D., & Jere, N. (2024). Deep learning for credit card fraud detection: A review of algorithms, challenges, and solutions. *IEEE Access*.
- [3]. Alarfaj, F. K., Malik, I., Khan, H. U., Almusallam, N., Ramzan, M., & Ahmed, M. (2022). Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms. *IEEE Access*, 10, 39700-39715.



- [4]. Khalid, A. R., Owoh, N., Uthmani, O., Ashawa, M., Osamor, J., & Adejoh, J. (2024). Enhancing credit card fraud detection: an ensemble machine learning approach. *Big Data and Cognitive Computing*, 8(1), 6.
- [5]. Alfaiz, N. S., & Fati, S. M. (2022). Enhanced credit card fraud detection model using machine learning. *Electronics*, 11(4), 662.
- [6]. Esenogho, E., Mienye, I. D., Swart, T. G., Aruleba, K., & Obaido, G. (2022). A neural network ensemble with feature engineering for improved credit card fraud detection. *IEEE access*, 10, 16400-16407.
- [7]. Ileberi, E., Sun, Y., & Wang, Z. (2022). A machine learning based credit card fraud detection using the GA algorithm for feature selection. *Journal of Big Data*, 9(1), 24.
- [8]. Asha, R. B., & KR, S. K. (2021). Credit card fraud detection using artificial neural network. *Global Transitions Proceedings*, 2(1), 35-41.
- [9]. Cherif, A., Badhib, A., Ammar, H., Alshehri, S., Kalkatawi, M., & Imine, A. (2023). Credit card fraud detection in the era of disruptive technologies: A systematic review. *Journal of King Saud University-Computer and Information Sciences*, 35(1), 145-174.
- [10]. Ileberi, E., Sun, Y., & Wang, Z. (2021). Performance evaluation of machine learning methods for credit card fraud detection using SMOTE and AdaBoost. *IEEE Access*, 9, 165286-165294.
- [11]. Tiwari, P., Mehta, S., Sakhuja, N., Kumar, J., & Singh, A. K. (2021). Credit card fraud detection using machine learning: a study. *arXiv preprint arXiv:2108.10005*.
- [12]. Chen, J. I. Z., & Lai, K. L. (2021). Deep convolutional neural network model for credit-card fraud detection and alert. *Journal of Artificial Intelligence*, 3(02), 101-112.
- [13]. Gupta, P., Varshney, A., Khan, M. R., Ahmed, R., Shuaib, M., & Alam, S. (2023). Unbalanced credit card fraud detection data: A machine learning-oriented comparative study of balancing techniques. *Procedia Computer Science*, 218, 2575-2584.
- [14]. Mienye, I. D., & Sun, Y. (2023). A deep learning ensemble with data resampling for credit card fraud detection. *IEEE Access*, 11, 30628-30638.
- [15]. Van Belle, R., Baesens, B., & De Weerd, J. (2023). CATCHM: A novel network-based credit card fraud detection method using node representation learning. *Decision Support Systems*, 164, 113866.
- [16]. Benchaji, I., Douzi, S., El Ouahidi, B., & Jaafari, J. (2021). Enhanced credit card fraud detection based on attention mechanism and LSTM deep model. *Journal of Big Data*, 8, 1-21.
- [17]. Yu, C., Xu, Y., Cao, J., Zhang, Y., Jin, Y., & Zhu, M. (2024, August). Credit card fraud detection using advanced transformer model. In *2024 IEEE International Conference on Metaverse Computing, Networking, and Applications (MetaCom)* (pp. 343-350).
- [18]. Novian, T. R., Idroes, G. M., Maulana, A., Hardi, I., Ringga, E. S., & Idroes, R. (2023). Credit card fraud detection for contemporary financial management using XGBoost-driven machine learning and data augmentation techniques. *Indatu Journal of Management and Accounting*, 1(1), 29-35.
- [19]. Jovanovic, D., Antonijevic, M., Stankovic, M., Zivkovic, M., Tanaskovic, M., & Bacanin, N. (2022). Tuning machine learning models using a group search firefly algorithm for credit card fraud detection. *Mathematics*, 10(13), 2272.
- [20]. Xiang, S., Zhu, M., Cheng, D., Li, E., Zhao, R., Ouyang, Y., ... & Zheng, Y. (2023, June). Semi-supervised credit card fraud detection via attribute-driven graph representation. In *Proceedings of the AAAI Conference on Artificial Intelligence* (Vol. 37, No. 12, pp. 14557-14565).
- [21]. Mniai, A., Tarik, M., & Jebbari, K. (2023). A novel framework for credit card fraud detection. *IEEE Access*, 11, 112776-112786.
- [22]. Abdul Salam, M., Fouad, K. M., Elbably, D. L., & Elsayed, S. M. (2024). Federated learning model for credit card fraud detection with data balancing techniques. *Neural Computing and Applications*, 36(11), 6231-6256.
- [23]. Salekshahrezaee, Z., Leevy, J. L., &



- Khoshgoftaar, T. M. (2023). The effect of feature extraction and data sampling on credit card fraud detection. *Journal of Big Data*, 10(1), 6.
- [24]. Zhu, M., Zhang, Y., Gong, Y., Xu, C., & Xiang, Y. (2024). Enhancing credit card fraud detection a neural network and smote integrated approach. *arXiv preprint arXiv:2405.00026*.
- [25]. Jiang, S., Dong, R., Wang, J., & Xia, M. (2023). Credit card fraud detection based on unsupervised attentional anomaly detection network. *Systems*, 11(6), 305.
- [26]. Malik, E. F., Khaw, K. W., Belaton, B., Wong, W. P., & Chew, X. (2022). Credit card fraud detection using a new hybrid machine learning architecture. *Mathematics*, 10(9), 1480.
- [27]. Habibpour, M., Gharoun, H., Mehdipour, M., Tajally, A., Asgharnezhad, H., Shamsi, A., ... & Nahavandi, S. (2023). Uncertainty-aware credit card fraud detection using deep learning. *Engineering Applications of Artificial Intelligence*, 123, 106248.
- [28]. Alharbi, A., Alshammari, M., Okon, O. D., Alabrah, A., Rauf, H. T., Alyami, H., & Meraj, T. (2022). A novel text2IMG mechanism of credit card fraud detection: A deep learning approach. *Electronics*, 11(5), 756.
- [29]. Lin, T. H., & Jiang, J. R. (2021). Credit card fraud detection with autoencoder and probabilistic random forest. *Mathematics*, 9(21), 2683.
- [30]. Singh, A., Ranjan, R. K., & Tiwari, A. (2022). Credit card fraud detection under extreme imbalanced data: a comparative study of data-level algorithms. *Journal of Experimental & Theoretical Artificial Intelligence*, 34(4), 571-598.